



One Hundred Eighteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

April 25, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528

Dear Ms. Easterly:

We write to inquire about the Cybersecurity and Infrastructure Security Agency's (CISA) reported plans to establish a new program office to identify "systemically important entities" (SIE) by the end of September.¹

Per your remarks at the March 21st Cybersecurity Advisory Committee meeting, we understand you hope to work with each sector risk management agency (SRMA) to identify SIEs in each of the 16 critical infrastructure sectors. Given the vast scope of this initiative, and its similarities to other programs previously initiated, we request additional information on CISA's proposed SIE designation efforts. Specifically, we request information on how these efforts complement or replace existing efforts to mitigate systemic risk to Section 9 entities, secure National Critical Functions (NCF), prioritize assets through the National Critical Infrastructure Prioritization Program, and maintain a National Asset Database. We also hope to understand how the National Risk Management Center (NRMCC) and the proposed new SIE office will coordinate and deconflict efforts related to SIEs.

Over the past decade, the federal government has undertaken multiple lines of effort to identify and mitigate risk to functions vital to U.S. national security, national economic security, and national public health and safety. In February 2013, Section 9 of *Executive Order (EO) 13636-Improving Critical Infrastructure Cybersecurity* directed the Department of Homeland Security (DHS), in coordination with relevant SRMAs, to annually identify and maintain a list of critical infrastructure entities where a cyber incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.² In May 2017, *EO 13800-Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* strengthened federal efforts to support the cybersecurity efforts of those designated Section 9 entities.³ In 2018, DHS established the NRMCC, which subsequently

¹Justin Doubleday, *CISA establishing 'systemically important entities' office*, FEDERAL NEWS NETWORK (March 23, 2023), <https://federalnewsnetwork.com/cybersecurity/2023/03/cisa-establishing-systemically-important-entities-office/>.

² EXECUTIVE OFFICE OF THE PRESIDENT, EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2013), <https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity>.

³ EXECUTIVE OFFICE OF THE PRESIDENT, EXECUTIVE ORDER 13800: STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE (2017),

published its initial set of NCFs to drive a more systematic approach to risk management activity across sectors.⁴ We also understand that some SRMAs, like the Departments of Energy and Treasury, may even maintain their own risk management designations completely independent of CISA's work, consistent with their obligations under section 9002(c)(2) of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*. We would like to understand the relationship between these existing efforts, spanning multiple Administrations, and CISA's proposed new SIE office and designation criteria.

Stakeholders across sectors seem to agree that identification and prioritization of systemic risk is critical to mitigating cyber threats. However, the task of identifying our nation's most critical assets is no small feat, and any effort to do so should be informed by—but not duplicative of—past efforts. CISA must have clear goals, objectives, and metrics to measure success in place at the outset. Last month, the Bank Policy Institute (BPI) formally testified in front of the subcommittee that, "Financial institutions are very supportive of efforts to identify and prioritize critical infrastructure assets that are most important to our national security. However, CISA should clarify what it intends to accomplish with a new designation and how it relates to existing efforts, including the Section 9 list, national critical functions and sector specific systemic risk designations like [systemically important financial institutions]." BPI went on to say, "Past proposals to create an SIE...designation would have duplicated existing designations and requirements on financial institutions, diverting resources from defending against threats to regulatory compliance."⁵ Government bureaucracy should not amount to increased risk for these entities. We intend to ensure all sectors, including financial services, are not tasked with duplicative designations and requirements with this proposed new program office.

We request a briefing from CISA to elaborate on the proposed new SIE office and how it plans to interface with the NRMC, especially as the NRMC welcomes new leadership. Such a briefing shall include, at a minimum:

1. A description of the goals of the new SIE office, including interim milestones;
2. A detailed description of the planned new SIE program office, including structure, estimated staff levels, and necessary resources.
3. How the new program office would integrate with, inform, and complement other ongoing designation schemes at CISA including but not limited to the Section 9 list, the National Critical Functions, and the National Critical Infrastructure Prioritization Program.
4. How the new program office plans to incorporate efforts from other SRMAs and other stakeholders within each sector.

Please provide this briefing no later than May 12, 2023.

<https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure>.

⁴ CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, NATIONAL CRITICAL FUNCTIONS, <https://www.cisa.gov/national-critical-functions#:~:text=CISA%2C%20through%20the%20National%20Risk,more%E2%80%94to%20these%20important%20functions>.

⁵ *CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective: Hearing Before the Subcommittee on Cybersecurity and Infrastructure Protection of the H. Comm. On Homeland Sec., 118th Cong. (March 23, 2023) (statement of Heather Hogsett, Senior Vice President, Technology and Risk Strategy for BITS, the Technology Policy Division of the Bank Policy Institute).*

Director Easterly
April 25, 2023
Page 3

Sincerely,

A handwritten signature in blue ink, appearing to read "Andrew R. Garbarino".

ANDREW R. GARBARINO
Chairman
Subcommittee on Cybersecurity and
Infrastructure Protection

A handwritten signature in blue ink, appearing to read "Eric Swalwell".

ERIC SWALWELL
Ranking Member
Subcommittee on Cybersecurity and
Infrastructure Protection